ON THE NUMBER OF LINEAR FORMS IN LOGARITHMS

Youness Lamzouri

Abstract. Let n be a positive integer. In this paper we estimate the size of the set of linear forms $b_1 \log a_1 + b_2 \log a_2 + ... + b_n \log a_n$, where $|b_i| \leq B_i$ and $1 \leq a_i \leq A_i$ are integers, as $A_i, B_i \to \infty$.

1. Introduction

The theory of linear forms in logarithms, developed by A. Baker ([1] and [2]) in the 60's, is a powerful method in the transcendental number theory. It consists of finding lower bounds for $|b_1 \log a_1 + b_2 \log a_2 + ... + b_n \log a_n|$, where the b_i are integers and the a_i are algebraic numbers for which $\log a_i$ are linearly independent over $\mathbb{Q}$. We consider the simpler case where the $a_i > 0$ are integers, and we let $B_j = \max\{|b_j|, 1\}$, and $B = \max_{1\leq j\leq n} B_j$.
Lang and Waldschmidt [4] conjectured the following

Conjecture. *Let $\epsilon > 0$. There exists $C(\epsilon) > 0$ depending only on ϵ, such that*

$$|b_1 \log a_1 + b_2 \log a_2 + ... + b_n \log a_n| > \frac{C(\epsilon)^n B}{(B_1...B_n a_1...a_n)^{1+\epsilon}}.$$

One part of the argument they used to motivate the Conjecture, is that the number of distinct linear forms $b_1 \log a_1 + b_2 \log a_2 + ... + b_n \log a_n$, where $|b_j| \leq B_j$ and $0 < a_j \leq A_j$, is $\asymp B_1...B_n A_1...A_n$, if the A_i and the B_i are sufficiently large.
In this paper we estimate the number of these linear forms as $A_i, B_i \to \infty$.
An equivalent formulation of the problem is to estimate the size of the following set

$$R = R(A_1, ..., A_n, B_1, ..., B_n) := \{r \in \mathbb{Q} : r = a_1^{b_1} a_2^{b_2} ... a_n^{b_n}, 1 \leq a_i \leq A_i, |b_i| \leq B_i\},$$

as $A_i, B_i \to \infty$.
For the easier case $A_i = A$ and $B_i = B$ for all i, a trivial upper bound on $|R|$ is $2^n A^n B^n / n! + o(A^n B^n)$, since permuting the numbers $a_i^{b_i}$ gives rise to the same number r. We prove that this bound is attained asymptotically as $A, B \to \infty$. Also we deal with the general case, which is harder since not every permutation is allowed for all the ranges. Indeed the size of R depends on the ranges of the A_i and the B_i, as we shall see in Corollaries 1 and 2.

Let $E \subset \{(a_1, ..., a_n, b_1, ..., b_n), 1 \leq a_i \leq A_i, |b_i| \leq B_i\}$. We say that $r \in \mathbb{Q}$ has a representation in E, if $r = a_1^{b_1} a_2^{b_2} ... a_n^{b_n}$, for some $(a_1, ..., a_n, b_1, ..., b_n) \in E$.

For $r \in R$, if $\sigma \in S_n$ satisfies $1 \le a_{\sigma(i)} \le A_i$, and $|b_{\sigma(i)}| \le B_i$ for all i, we say that σ permutes r, or σ is a possible permutation for the $a_i^{b_i}$. Finally we say that a permutation $\sigma \in S_n$ is permissible if

$$|\{r \in R : \sigma \text{ permutes } r\}| \gg A_1...A_nB_1...B_n.$$

The main result of this paper is the following

Theorem. *There exists a set* $E \subset \{(a_1, ..., a_n, b_1, ..., b_n), 1 \le a_i \le A_i, |b_i| \le B_i\}$ *satisfying*

$$|E| \sim 2^n A_1A_2...A_nB_1B_2...B_n,$$

as $A_i, B_i \to \infty$, *such that any rational number* $r \in \{a_1^{b_1}a_2^{b_2}...a_n^{b_n} : (a_1, ..., a_n, b_1, ..., b_n) \in E\}$ *has a unique representation in* E *up to permissible permutations.*

From this result we can deduce that $|R|$ is asymptotic to the cardinality of the set of $2n$-tuples $\{(a_1, ..., a_n, b_1, ..., b_n), 1 \le a_i \le A_i, |b_i| \le B_i\}$ modulo permissible permutations. In the case $A_i = A$, $B_i = B$, every permutation is permissible and we deduce the following Corollary

Corollary 1. *As* $A, B \to \infty$, *we have*

$$|\{r \in \mathbb{Q} : r = a_1^{b_1}a_2^{b_2}...a_n^{b_n}, 1 \le a_i \le A, |b_i| \le B\}| = \frac{2^nA^nB^n}{n!} + o(A^nB^n).$$

Now suppose that $A_i = o(A_{i+1})$ for all $1 \le i \le n-1$, or $B_i = o(B_{i+1})$ for all $1 \le i \le n-1$. For a non-identity permutation $\sigma \in S_n$, there exists j for which $\sigma(j) \ne j$. Therefore if σ permutes $r = a_1^{b_1}a_2^{b_2}...a_n^{b_n}$, we must have $1 \le a_j, a_{\sigma(j)} \le \min(A_j, A_{\sigma(j)})$ and $-\min(B_j, B_{\sigma(j)}) \le b_j, b_{\sigma(j)} \le \min(B_j, B_{\sigma(j)})$. And so we deduce that

$$\begin{aligned} &|\{r \in \mathbb{Q} : r = a_1^{b_1}a_2^{b_2}...a_n^{b_n}, 1 \le a_i \le A_i, |b_i| \le B_i : \sigma \text{ permutes } r\}| \\ &\le 2^nA_1...A_nB_1...B_n\left(\frac{\min(A_j, A_{\sigma(j)})\min(B_j, B_{\sigma(j)})}{\max(A_j, A_{\sigma(j)})\max(B_j, B_{\sigma(j)})}\right) = o(A_1...A_nB_1...B_n), \end{aligned}$$

by our assumption on the A_i and B_i. Thus in this case no permutation $\sigma \ne 1$ is permissible. Therefore we have

Corollary 2. *If* $A_i = o(A_{i+1})$ *for all* $1 \le i \le n-1$, *or* $B_i = o(B_{i+1})$ *for all* $1 \le i \le n-1$, *then*

$$|\{r \in \mathbb{Q} : r = a_1^{b_1}a_2^{b_2}...a_n^{b_n}, 1 \le a_i \le A_i, |b_i| \le B_i\}| \sim 2^nA_1...A_nB_1...B_n,$$

as $A_i, B_i \to \infty$.

We can observe that Corollaries 1 and 2 correspond to extreme cases: in Corollary 1 all permutations are permissible, while none is permissible in Corollary 2. Indeed we can prove

Corollary 3. *As $A_i, B_i \to \infty$, we have*

$$\frac{2^n}{n!} A_1 ... A_n B_1 ... B_n \lesssim |R| \lesssim 2^n A_1 ... A_n B_1 ... B_n.$$

Moreover the two bounds are optimal.

Proof. From the Theorem we have that

$$|R| \sim \sum_{\substack{1 \le a_1 \le A_1 \\ |b_1| \le B_1}} ... \sum_{\substack{1 \le a_n \le A_n \\ |b_n| \le B_n}} \frac{1}{|\{\sigma \in S_n : \sigma \text{ is possible for the } a_i^{b_i}\}|}.$$

The result follows from the fact that $1 \le |\{\sigma \in S_n : \sigma \text{ is possible for the } a_i^{b_i}\}| \le n!$.

For the simple case $n = 2$, there is only one non-trivial permutation $\sigma = (12)$. This permutation is possible only if $1 \le a_1, a_2 \le \min(A_1, A_2)$ and $|b_1|, |b_2| \le \min(B_1, B_2)$. Then by the Theorem, and after a simple calculation we deduce that

$$\begin{aligned} &|\{r \in \mathbb{Q} : r = a_1^{b_1} a_2^{b_2}, 1 \le a_1 \le A_1, 1 \le a_2 \le A_2, |b_1| \le B_1, |b_2| \le B_2\}| \\ &\sim 4A_1A_2B_1B_2 - 2\min(A_1, A_2)^2 \min(B_1, B_2)^2. \end{aligned}$$

In general the size of $|R|$ is asymptotic to an homogeneous polynomial of degree $2n$ in the variables $A_1, ..., A_n, B_1, ..., B_n$. Moreover it's also necessary to order the A_i's and B_i's, so without loss of generality we assume that $A_1 \le A_2 \le ... \le A_n$ and $B_{\pi(1)} \le B_{\pi(2)} \le ... \le B_{\pi(n)}$, where $\pi \in S_n$ is a permutation.
We prove the following

Proposition. *Suppose that $A_1 \le A_2 \le ... \le A_n$ and $B_{\pi(1)} \le B_{\pi(2)} \le ... \le B_{\pi(n)}$, where $\pi \in S_n$ is a permutation. Also let $A_0 = B_{\pi(0)} = 1$.*
Then $|R|$ is asymptotic to

$$2^n \sum_{\substack{i_1 = 1 \\ 1 \le j_1 \le \pi^{-1}(1)}} \sum_{\substack{1 \le i_2 \le 2 \\ 1 \le j_2 \le \pi^{-1}(2)}} ... \sum_{\substack{1 \le i_n \le n \\ 1 \le j_n \le \pi^{-1}(n)}} \frac{\prod_{k=1}^n (A_{i_k} - A_{i_k - 1})(B_{\pi(j_k)} - B_{\pi(j_k - 1)})}{|\{\sigma \in S_n : i_{\sigma(l)} \le l, j_{\sigma(l)} \le \pi^{-1}(l), \forall 1 \le l \le n\}|},$$

as $A_i, B_i \to \infty$.

Acknowledgments.
I sincerely thank my advisor, Professor Andrew Granville, for suggesting the problem, for many valuable discussions, and for his encouragement during the various stages of this work.

2. Preliminary lemmas

Let C be a positive real number. We say that the n-tuple $(a_1, ..., a_n)$ satisfies condition (1_C), if there exists a prime p, such that $p^k | a_1 a_2 ... a_n$ where $k \geq 2$, and $p^k \geq C$.

Lemma 1. *We have*

$$|\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : \textit{which satisfy } (1_C)\}| \ll_n \frac{A_1 ... A_n (\log C)^n}{\sqrt{C}}.$$

Proof. First we have

$$\begin{aligned} &|\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : \text{which satisfy } (1_C)\}| \\ &\leq \sum_p |\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : \exists k \geq 2, p^k \geq C, \text{and } p^k | a_1 a_2 ... a_n\}|. \end{aligned} \tag{1}$$

Case 1. $p \leq \sqrt{C}$
In this case pick k to be the smallest integer such that $p^k \geq C$, ie $k = [\log C / \log p] + 1$. Then the number of $(a_1, ..., a_n)$ such that $p^k | a_1 a_2 ... a_n$ is equal to

$$\sum_{d_1 d_2 ... d_n = p^k} \prod_{i=1}^{n} \sum_{\substack{1 \leq a_i \leq A_i \\ d_i | a_i}} 1 \leq d_n(p^k) \frac{A_1 ... A_n}{p^k} \leq d_n(p^k) \frac{A_1 ... A_n}{C}.$$

Now $d_n(p^k) = \binom{n+k-1}{k}$, and by Stirling's formula, for k large enough we have

$$\begin{aligned} \log d_n(p^k) &= (n + k - 1 + \frac{1}{2}) \log(n + k - 1) - (k + \frac{1}{2}) \log k - (n - 1 + \frac{1}{2}) \log(n - 1) + O(1) \\ &\leq (k + \frac{1}{2}) \log \left(1 + \frac{n-1}{k}\right) + (n - \frac{1}{2}) \log \left(\frac{n - 1 + k}{n - 1}\right) \\ &\leq n \log k. \end{aligned}$$

Then summing over these primes gives

$$\sum_{p \leq \sqrt{C}} |\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : p^k | a_1 a_2 ... a_n\}| = O_n \left(\frac{A_1 ... A_n (\log C)^n}{\sqrt{C}}\right). \tag{2}$$

Case 2. $p > \sqrt{C}$
In this case pick $k = 2$. Then the number of $(a_1, ..., a_n)$ such that $p^2 | a_1 a_2 ... a_n$ is $O(A_1 ... A_n / p^2)$, where the constant involved in the O depends only on n. Therefore summing over these primes gives

$$\sum_{p > \sqrt{C}} |\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : p^2 | a_1 a_2 ... a_n\}| = O_n \left(\frac{A_1 ... A_n}{\sqrt{C}}\right). \tag{3}$$

Thus combining (1), (2) and (3) gives the result.

We say that $(a_1, ..., a_n)$ satisfies condition (2_C) if at least one of the a_i is C-smooth: that is has all its prime factors lying below C.

Lemma 2. *Write $C^{u_i} = A_i$ for all $1 \leq i \leq n$. Then uniformly for $\min_{1\leq i\leq n} A_i \geq C \geq 2$, we have*

$$|\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : \textit{which satisfy } (2_C)\}| \ll_n A_1A_2...A_n \left(\sum_{i=1}^{n} e^{-u_i/2}\right).$$

Proof. We have that

$$|\{(a_1, ..., a_n), 1 \leq a_i \leq A_i : \text{which satisfy } (2_C)\}| \ll_n A_1A_2...A_n \sum_{i=1}^{n} \frac{\Psi(A_i, C)}{A_i},$$

where $\Psi(x, y)$ is the number of y-smooth positive integers below x. The result follows by the following Theorem of de Bruijn [3]

$$\Psi(A_i, C) \ll A_i e^{-u_i/2},$$

uniformly for $A_i \geq C \geq 2$.

We say that $(b_1, b_2, ..., b_n)$ satisfy condition (3_C), if there exists an n-tuple of integers $|c_i| \leq 2\log C$ not all zero, such that $c_1b_1 + c_2b_2 + ... + c_nb_n = 0$.

Lemma 3. *We have that*

$$|\{(b_1, ..., b_n), |b_i| \leq B_i : \textit{which satisfy condition } (3_C)\}| \leq B_1B_2...B_n \sum_{i=1}^{n} \left(\frac{(9\log C)^n}{B_i}\right).$$

Proof. We note that

$$\begin{aligned}
&|\{(b_1, ..., b_n), |b_i| \leq B_i : \text{which satisfy condition } (3_C)\}| \\
&\leq \sum_{\substack{|c_i|\leq 2\log C \\ (c_1,...,c_n)\neq(0,...,0)}} |\{(b_1, ..., b_n), |b_i| \leq B_i : c_1b_1 + c_2b_2 + ... + c_nb_n = 0\}| \\
&\leq \sum_{\substack{|c_i|\leq 2\log C \\ (c_1,...,c_n)\neq(0,...,0)}} (2B_1 + 1)...(2B_n + 1) \sum_{i=1}^{n} \left(\frac{1}{2B_i + 1}\right) \leq B_1B_2...B_n \sum_{i=1}^{n} \left(\frac{(9\log C)^n}{B_i}\right).
\end{aligned}$$

3. Proof of the results

Proof of the Theorem. We begin by choosing $C := \min(B_1, ..., B_n, \log A_1, ..., \log A_n)$. We consider the following set

$$\begin{aligned}
E :=&\{(a_1, ..., a_n, b_1, ..., b_n), 1 \leq a_i \leq A_i, |b_i| \leq B_i : \\
&(a_i) \text{ don't satisfy any of } (1_C),(2_C),\ (b_i) \text{ don't satisfy } (3_C)\}.
\end{aligned}$$

Then by our choice of C, if we combine Lemmas 1, 2 and 3, we observe that $|E| = 2^n A_1...A_n B_1...B_n(1+o(1))$.
Therefore it remains to prove that any representation of a rational number r as $a_1^{b_1}a_2^{b_2}...a_n^{b_n}$ where $(a_1,...,a_n,b_1,...,b_n)$ belongs to E, is unique up to possible permutations of the $a_i^{b_i}$, and finally we can consider only permissible permutations (since the number of $r \in R$ which can be permuted by a non-permissible permutation is negligible).
We begin by considering the following equation

$$a_1^{b_1}a_2^{b_2}...a_n^{b_n} = e_1^{f_1}e_2^{f_2}...e_n^{f_n}, \tag{4}$$

where $(a_1,...,a_n,b_1,...,b_n)$ and $(e_1,...,e_n,f_1,...,f_n)$ are in E. If for some i, a_i contains a prime factor p such that $p^2 \nmid a_1a_2...a_n$ and $p^2 \nmid e_1e_2...e_n$, then $b_i \in \{f_1,f_2,...f_n\}$. Now suppose that there exists $1 \le j \le n$ such that $b_j \notin \{f_1,f_2,...f_n\}$, then for all the primes p that divides a_j, there exists $k \ge 2$ for which $p^k|a_1a_2...a_n$ or $p^k|e_1e_2...e_n$, but the (a_i) and the (e_i) don't satisfy condition (1_C) and so we must have $p^k \le C$, which implies that a_j is C-smooth; however this contradicts the fact that the (a_i) do not satisfy condition (2_C). Therefore we deduce that

$$\{b_1,b_2,...,b_n\} = \{f_1,f_2,...,f_n\}.$$

Then up to permutations, we have that $b_i = f_i$, and so equation (4) become

$$a_1^{b_1}a_2^{b_2}...a_n^{b_n} = e_1^{b_1}e_2^{b_2}...e_n^{b_n}. \tag{5}$$

Let p be any prime dividing $a_1a_2...a_n$, and let $\alpha_i \ge 0$ and $\beta_i \ge 0$ be the corresponding powers of p in a_i and e_i respectively, and let $c_i = \alpha_i - \beta_i$. Then equation (5) implies that

$$c_1b_1 + c_2b_2 + ...c_nb_n = 0.$$

Now the (a_i) and the (e_i) do not satisfy condition (1_C), and so $0 \le \alpha_i, \beta_i \le \log C/\log 2 \le 2\log C$, which implies that $|c_i| \le 2\log C$. And since the (b_i) do not satisfy condition (3_C), we deduce that $c_i = 0$, and then $\alpha_i = \beta_i$ for all $1 \le i \le n$. Since this is true for every prime factor of $a_1a_2...a_n$, we must have $a_i = e_i$ for all $1 \le i \le n$, and our Theorem is proved.

Proof of the Proposition. We want to count the number of elements $r = (r_1,...,r_n)$, where $r_i = (a_i,b_i) \in [1,A_i] \times [-B_i,B_i] \cap \mathbb{Z} \times \mathbb{Z}$, modulo possible permutations of the r_i's.
Since the number of r for which some b_i is 0, is $o(A_1...A_nB_1...B_n)$, we can suppose that all the b_i's are positive by symmetry.
Moreover let $R_i := [1,A_i] \times [1,B_i] \cap \mathbb{Z} \times \mathbb{Z}$, and define the following distinct discrete sets $R_{ij} := [A_{i-1},A_i] \times [B_{\pi(j-1)},B_{\pi(j)}] \cap \mathbb{Z} \times \mathbb{Z}$, for $1 \le i,j \le n$.
For every $1 \le k \le n$, we have

$$R_k = \bigsqcup_{\substack{1 \le i_k \le k \\ 1 \le j_k \le \pi^{-1}(k)}} R_{i_kj_k}. \tag{6}$$

This implies

$$R_1 \times R_2 \times ... \times R_n = \bigsqcup_{\substack{i_1=1\\ 1\le j_1\le \pi^{-1}(1)}} \bigsqcup_{\substack{1\le i_2\le 2\\ 1\le j_2\le \pi^{-1}(2)}} ... \bigsqcup_{\substack{1\le i_n\le n\\ 1\le j_n\le \pi^{-1}(n)}} R_{i_1j_1} \times R_{i_2j_2} \times ... \times R_{i_nj_n}.$$

Now consider the elements $r \in R_{i_1j_1} \times R_{i_2j_2} ... \times R_{i_nj_n}$, with $1 \le i_k \le k$ and $1 \le j_k \le \pi^{-1}(k)$ being fixed. If $\sigma \in S_n$ permutes r, then $r_{\sigma(k)} \in R_k$ for all $1 \le k \le n$, but $r_{\sigma(k)} \in R_{i_{\sigma(k)}j_{\sigma(k)}}$ also, which implies that $R_{i_{\sigma(k)}j_{\sigma(k)}} \bigcap R_k \neq \emptyset$. From (6) this is equivalent to $R_{i_{\sigma(k)}j_{\sigma(k)}} \subseteq R_k$, and thus to the fact that $i_{\sigma(k)} \le k$ and $j_{\sigma(k)} \le \pi^{-1}(k)$ for all $1 \le k \le n$. Therefore for any $r \in R_{i_1j_1} \times R_{i_2j_2} ... \times R_{i_nj_n}$, the number of $\sigma \in S_n$ which permutes r is constant and equal to

$$|\{\sigma \in S_n : i_{\sigma(l)} \le l, j_{\sigma(l)} \le \pi^{-1}(l), \forall 1 \le l \le n\}|.$$

Thus the number of elements in $R_1 \times R_2 ... \times R_n$, modulo possible permutations is

$$\sum_{\substack{i_1=1\\ 1\le j_1\le \pi^{-1}(1)}} \sum_{\substack{1\le i_2\le 2\\ 1\le j_2\le \pi^{-1}(2)}} ... \sum_{\substack{1\le i_n\le n\\ 1\le j_n\le \pi^{-1}(n)}} \frac{\prod_{k=1}^n (A_{i_k} - A_{i_k-1})(B_{\pi(j_k)} - B_{\pi(j_k-1)})}{|\{\sigma \in S_n : i_{\sigma(l)} \le l, j_{\sigma(l)} \le \pi^{-1}(l), \forall 1 \le l \le n\}|},$$

which implies the result.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers I*, Mathematika **13**, 1966, 204-216.

[2] ———, *Linear forms in the logarithms of algebraic numbers II, III*, Mathematika **14**, 1967, 102-107, 220-228.

[3] N.G. de Bruijn, *On the number of positive integers $\le x$ and free of prime factors $> y$. II*, Nederl. Akad. Wetensch. Proc. Ser. A **69**, 239-247= Indag. Math **28**, 1966, 239-247.

[4] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **231**. Springer-Verlag, Berlin-New York, 1978, xi+261 pp.

[5] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, **46**. Cambridge University Press, Cambridge, 1995, xvi+448 pp.

Départment de Mathématiques et Statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7, Canada

E-mail address: Lamzouri@dms.umontreal.ca